The **Allaple** Worm

Malware Analysis

. . .we anticipate that in the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats.

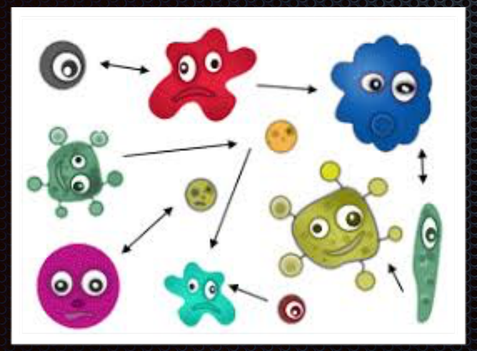
—FBI director James B. Comey, November 14, 2013[2]

Indeed, other sources of data support this dire conclusion. The UK insurance market, Lloyd's of London, estimated that cyberattacks cost businesses $400 billion globally per year.[3] In 2014, one billion records were compromised. This caused *Forbes* magazine to refer to 2014 as "The Year of the Data Breach."[3,8] Unfortunately, identifying 2014 as the year of the data breach may still prove to be premature. It could easily get worse.

Jordan Jones
Ryan Phillips
Tim Ellerbe
Vittal Siddaiah
Sachin Kusuma

Origin

- First sighting in 2006
- Polymorphic
- Spreads over the LAN and over to the Internet.
- Allaple was designed by a dissatisfied customer ***Arthur Boiko*** of an insurance company to DDOS some web sites in Estonia.



Polymorphic means that the worm morphs/changes its code with each stored copy for reproduction and propagation. This polymorphic behavior challenges the anti-virus software.

Impact

TOP 10 Windows malware 2015

1	ALLAPLE	17,315,842
2	SYTRO	5,318,628
3	VIRUT	4,898,268
4	RAMNIT	3,974,655
5	ELKERN	3,557,383
6	VIRLOCK	2,889,200
7	VB	2,007,596
8	AGENT	1,865,219
9	EXPIRO	1,768,984
10	VOBFUS	1,745,899

TOP 10 Windows malware Q1/Q2 2016

1	ALLAPLE	4,245,912
2	VIRUT	3,623,871
3	RAMNIT	2,976,489
4	VIRLOCK	1,534,457
5	AGENT	1,477,927
6	PARITE	1,147,433
7	SALITY	1,079,641
8	MIRA	882,365
9	LAMER	739,099
10	ZEGOST	616,975

Ref: AV-TEST_Security_Report_2015-2016.pdf

Technical Expose

Win32/Allaple.A

Seeks other machines across a network, and attempts to gain access in one of two ways

Exploiting weak logon passwords

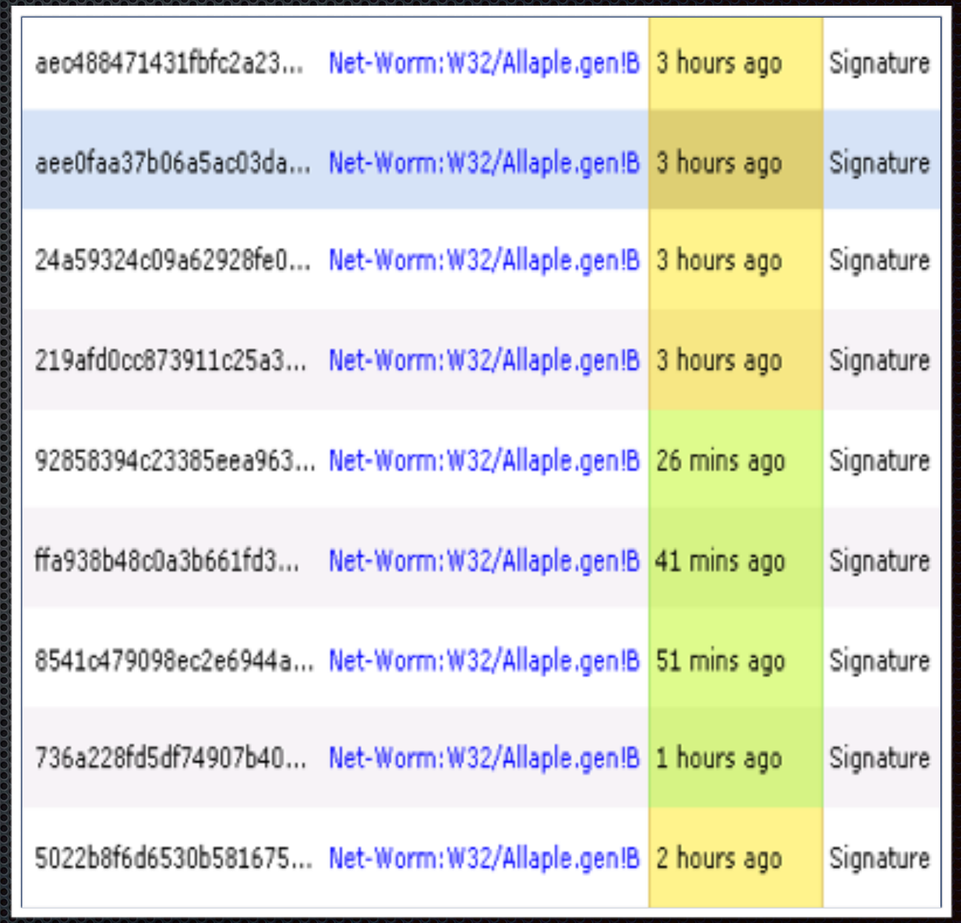
Dictionary attack to connect and logon to remote computers

***The Allaple Worm**, Malware Analysis*

Technical Expose

When executed, the worm launches several threads which accomplish different tasks simultaneously:

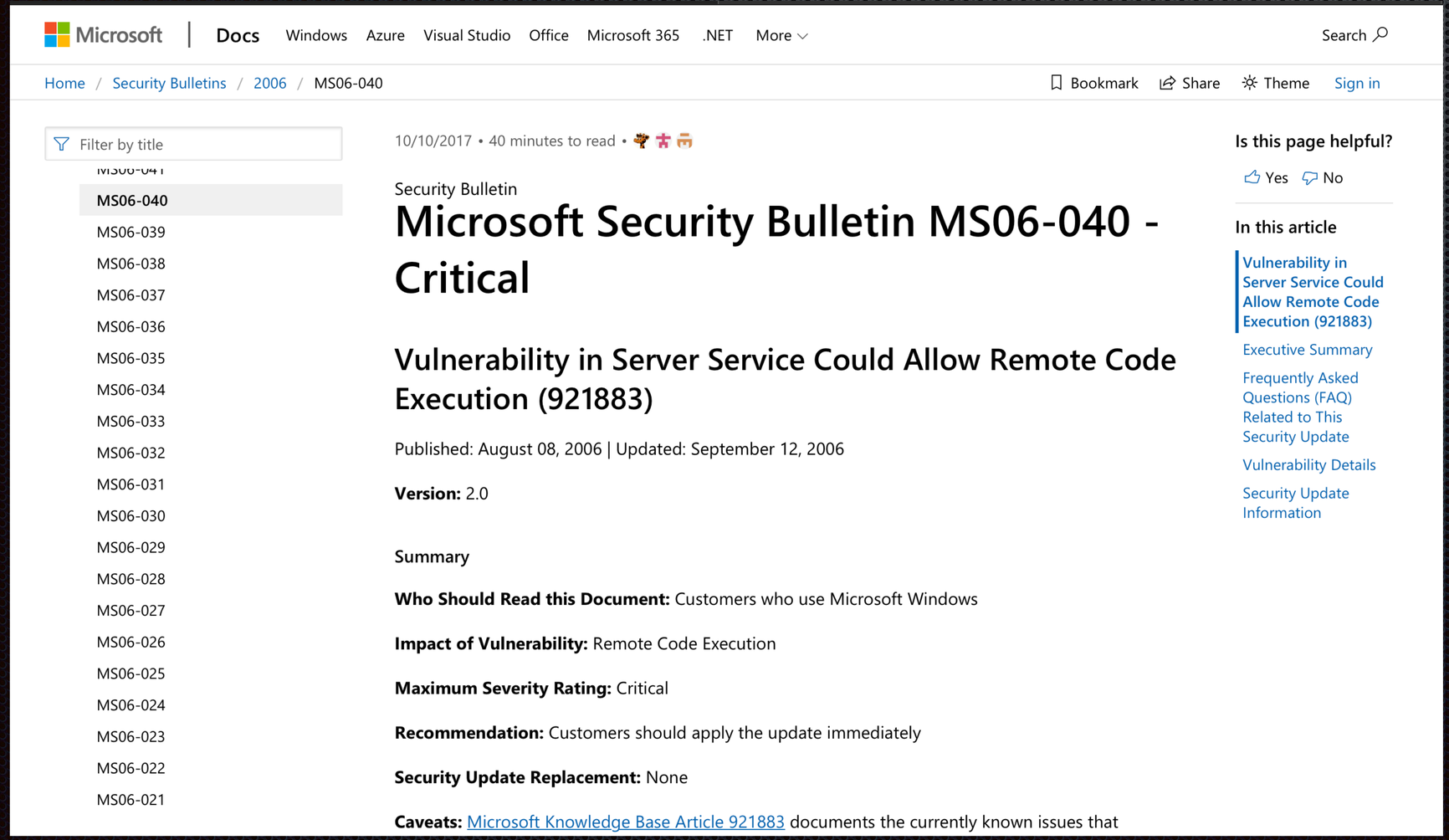
- DoS attack against a specific IP address.
  - *The worm sends an echo ping request and waiting for a response. Once it is received Allaple starts a DoS attack by flooding multiple network ports.*
- DoS attack against specific Web sites
  - *The worm attempts DoS attacks on three websites with a .ee domain suffix.*
- Infecting open shares across a network



aec488471431fbfc2a23...	Net-Worm:W32/Allaple.gen!B	3 hours ago	Signature
aee0faa37b06a5ac03da...	Net-Worm:W32/Allaple.gen!B	3 hours ago	Signature
24a59324c09a62928fe0...	Net-Worm:W32/Allaple.gen!B	3 hours ago	Signature
219afd0cc873911c25a3...	Net-Worm:W32/Allaple.gen!B	3 hours ago	Signature
92858394c23385eea963...	Net-Worm:W32/Allaple.gen!B	26 mins ago	Signature
ffa938b48c0a3b661fd3...	Net-Worm:W32/Allaple.gen!B	41 mins ago	Signature
8541c479098ec2e6944a...	Net-Worm:W32/Allaple.gen!B	51 mins ago	Signature
736a228fd5df74907b40...	Net-Worm:W32/Allaple.gen!B	1 hours ago	Signature
5022b8f6d6530b581675...	Net-Worm:W32/Allaple.gen!B	2 hours ago	Signature

Technical Expose

Exploiting computers not updated with **Microsoft Security Bulletin *MS06-040***



Microsoft | Docs Windows Azure Visual Studio Office Microsoft 365 .NET More Search

Home / Security Bulletins / 2006 / MS06-040 Bookmark Share Theme Sign in

Filter by title

MS06-040
MS06-039
MS06-038
MS06-037
MS06-036
MS06-035
MS06-034
MS06-033
MS06-032
MS06-031
MS06-030
MS06-029
MS06-028
MS06-027
MS06-026
MS06-025
MS06-024
MS06-023
MS06-022
MS06-021

10/10/2017 • 40 minutes to read •

Security Bulletin

Microsoft Security Bulletin MS06-040 - Critical

Vulnerability in Server Service Could Allow Remote Code Execution (921883)

Published: August 08, 2006 | Updated: September 12, 2006

Version: 2.0

Summary

Who Should Read this Document: Customers who use Microsoft Windows

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

Recommendation: Customers should apply the update immediately

Security Update Replacement: None

Caveats: Microsoft Knowledge Base Article 921883 documents the currently known issues that

Is this page helpful?

Yes No

In this article

Vulnerability in Server Service Could Allow Remote Code Execution (921883)
Executive Summary
Frequently Asked Questions (FAQ) Related to This Security Update
Vulnerability Details
Security Update Information

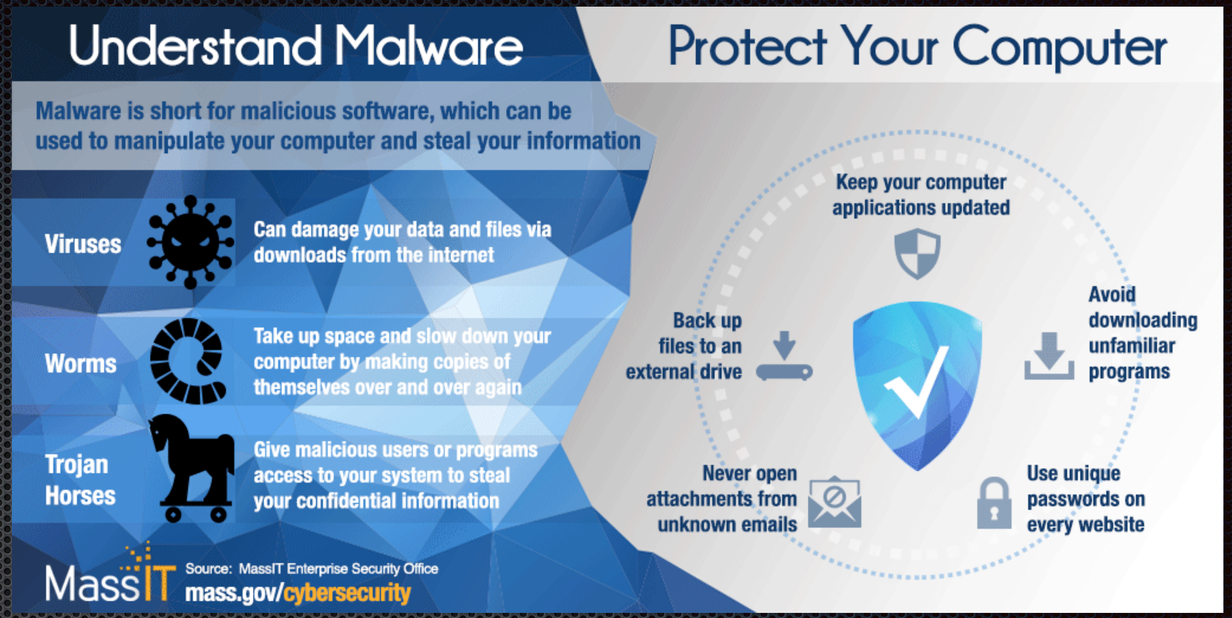
Containment Strategy

- Diagnosing the symptoms :Users infected often reported the famous pop-up in the bottom right hand corner of the Taskbar stating “Warning! Running trial version! Now running trial version of the software! Click here to purchase the full version of the software and get full protection for your PC!”
- System speed reduced
- Browser hijacking
- Unauthorized amendments to System-Settings
- Keyloggers
- Device Driver Update disabled
- Fake “Blue-Screen of Doom”
- Unusual Desktop short-cutsDoS attack against a specific IP address.

Resolution

- For Windows
  - Users the first step in removal procedure is to open Windows Task Manager, open the Process Option and terminate malicious scripts “bzehxvnz.exe, hwexrtne.exe, bnshhqj.exe, jjlenkbt.exe, tsbjbtvn.exe”.
  - Reboot in Safe Mode, extinguish Net-Worm.Win32.Allaple.a process. Locate the file Net-Worm.Win32.Allaple.a within the registry and delete it. Search for “bzehxvnz.exe, hwexrtne.exe, bnshhqj.exe, jjlenkbt.exe, tsbjbtvn.exe” and delete them as well. In theory, this may resolve the issues described above. For further safety measures it is advised to run a Malware-Scan along the lines of Spybot Search & Destroy to further remove any lingering problems.
- For Linux Users(Network Protection)
  - With the assistance of the Utility Snort run the following command. (This would be useful to determine infection across an entire network to locate each infected device)
  - alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET WORM Allaple ICMP Sweep Ping Outbound"; icode:0; itype:8; content:"Babcdefghijklmnopqrstuvwabcdefghi"; threshold: type both, count 1, seconds 60, track by_src; classtype:trojan-activity; reference:url,www.sophos.com/virusinfo/analyses/w32allapleb.html; reference:url,isc.sans.org/diary.html?storyid=2451; sid:2003292; rev:6;)
- This provides the admin with a comprehensive analysis of infection within a network, scanning for anomalies and malicious port activity.

Awareness Training



- Use **STRONG** passwords
- Use **non-admin** account unless necessary
- Be **vigilant** on links, attachments
- Do not **mount/attach** unfamiliar accessories unless from a reliable source
- Keep your **software up-to-date**

We are in a **vulnerable world**, and **we are responsible** for protecting your assets

The Allaple Worm, *Malware Analysis*

References

- https://www.f-secure.com/v-descs/allaple_a.shtml
- http://isc.sans.org/diary.html?storyid=2451
- http://www.sophos.com/virusinfo/analyses/w32allapleb.html